Digital Asset Redemption

DRK_MDR OPERATIVE

Operative

Managed detection and response for the dark web

DISARM THREATS AT THEIR SOURCE.

Your threat surface extends to the deepest parts of the dark web, but that doesn't mean you're powerless to protect it. DRK_MDR is the world's first managed detection and response platform for the dark web. Our operatives **have infiltrated the inner circles of the cyber criminal ecosystem**, giving you the power to counteract threats where they start.

WE RESPOND TO THREATS WHERE WE DETECT THEM: ON THE DARK WEB.

INFILTRATE

Think of us as your personal spy operation. Our operatives spend years building trusted identities that allow them to **infiltrate the dark web's most exclusive forums and marketplaces**.

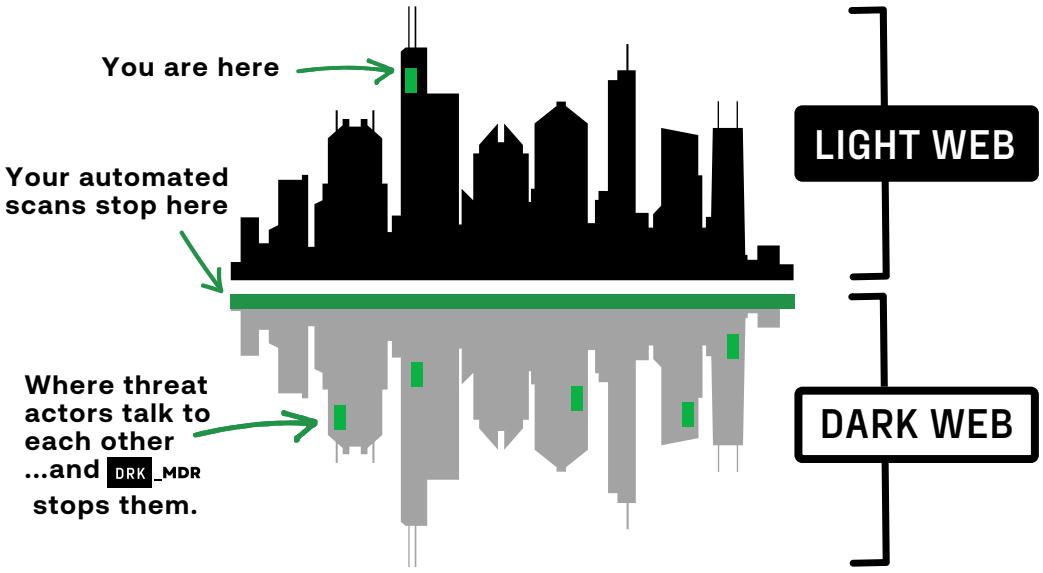
INTERCEPT

When operatives learn about your exposures, they listen. They work fast to **understand the who, what, where, when, and how of your exposure**. This intelligence gives you more options to contain the threat.

INTERDICT

When your potential exposures appear for sale, our operatives will qualify, contextualize, and **provide you with a COA (Course of Action)**. We can also take action such as purchasing leaked access or data on your behalf.

MANAGED DETECTION AND RESPONSE FOR THE DARK WEB



Digital Asset Redemption

DRK_MDR OPERATIVE

Operative

Don't just see the dark web. Respond there.

Traditional security tools and dark web monitoring look at what threat actors want you to see.

DRK_MDR shows you what they're hiding.

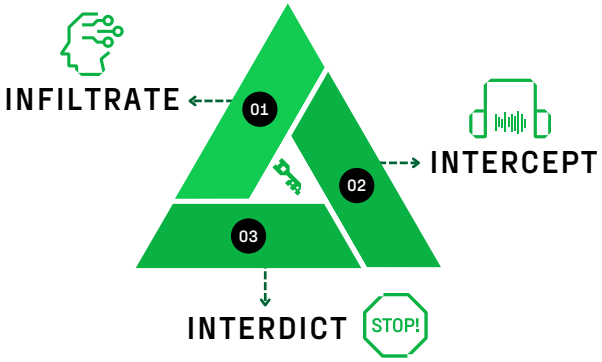
Established personas

The places where threat actors communicate aren't accessible to just anyone. It takes **years of establishing personas, engaging threat actors in the ways they engage each other, and building trust in the communities**.

Companies can't risk allowing their employees to engage in these types of dark web spaces and criminal communications for obvious legal and liability reasons.

Trained operatives

Understanding where to engage with threat actors is just the beginning. Forward-deployed intelligence operations also require **specific skills such as offensive security backgrounds and social engineering experience**. This experience helps the operatives frame engagements to elicit valuable responses and intelligence without arousing suspicion.



Payment options

Threat actors are quick to recognize "security researchers" who won't engage in their business dealings. The intelligence gathered from even a small cryptocurrency transaction can provide a boon of intelligence to the victim, incident response team, and law enforcement. With payment options at the ready, The DAR Team is able to **keep intelligence-gathering operations going, maintain threat actors' trust and confidence, and give victims both more and better options during their crisis.**

Operational security

Because undercover operations can put organizations at risk if not performed properly, The DAR Team **follows a strict operational security code**. Combined with a deep understanding of adversaries, these operational guardrails allow The DAR Team to **operate without putting victims at further risk.**

Digital Asset Redemption

DRK_MDR ENGAGE

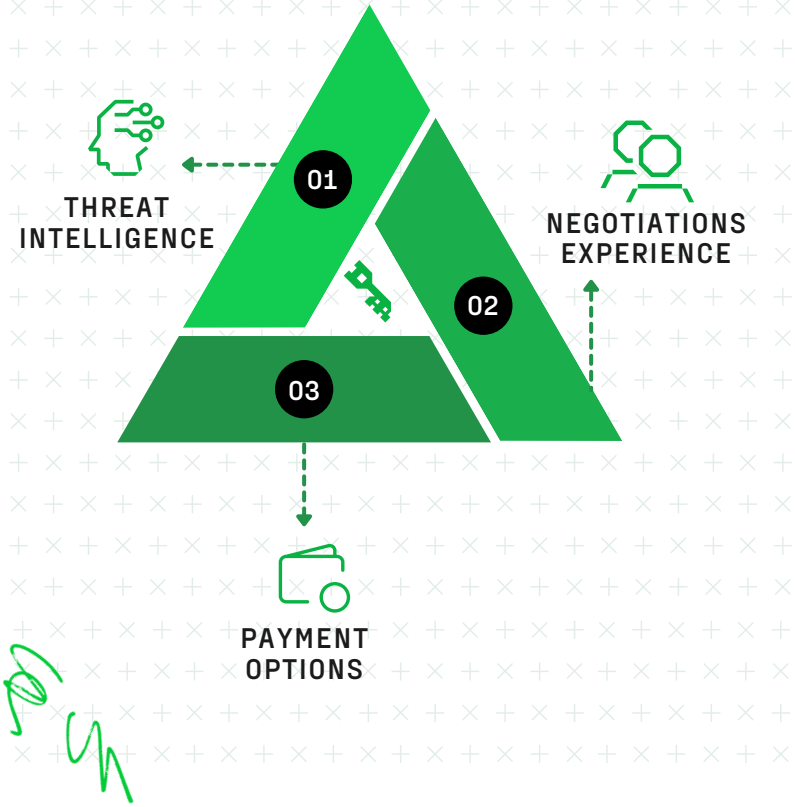
Engage

Negotiations and payment

CONFIDENTLY CONFRONT CYBERCRIME.

The middle of a crisis is a bad time to learn how to negotiate with criminals. DAR's ransomware response capabilities – our **Engage** services – gives you access to **negotiations experts and compliant payment services** in the event of an extortion event.

Our experienced **negotiators know how to communicate with, assess, and understand your extortionists**, resulting in an average 77% reduction in ransom demand while also giving IR teams more time to work.



UNSCRIPTED **NEGOTIATIONS.**

COMPLIANT **PAYMENTS.**

READY WHEN YOU ARE.

77%

AVG. REDUCTION IN RANSOM DEMANDS

MEET YOUR THREAT ACTOR NEGOTIATIONS TEAM.

"Negotiating with extortionists" probably isn't in your job description. And when your company is in the middle of a ransomware event, you need pros who do this full time.

With **over 4500 successful threat actor engagements** under our belt, our team of skilled negotiators guide you through the crisis and back to business – and back to your actual jobs.

Digital Asset Redemption

DRK_MDR ENGAGE

Engage

Don't just prepare for a breach. Prepare for recovery.

FACT: CRIMINALS DON'T TAKE CHECKS.

When you're in the position of needing to make a payment to a threat actor, there are a lot of questions you need to answer, but the most important one is: **Who am I paying?**

You need a payment provider who can **perform threat actor attribution, assess your sanctions risks, and keep your payments compliant**.

- CRYPTO WALLET MANAGEMENT
- SANCTIONS AND COMPLIANCE SCREENS
- OPEN DIALOGUE WITH AUTHORITIES

INTELLIGENCE

Embedded operatives inform your negotiations and compliant payment options.

NEGOTIATIONS

Social engineers and expert negotiators work to take you from event to recovery.

COMPLIANCE

Informed attribution to keep you inside evolving sanctions and legal standards.

IN YOUR BACK POCKET

DAR's Engage ensures your incident response plan will include **priority extortion negotiation and payment services** in the event of an attack.

- **Engage threat actors with precision**
- **More (and better!) options in a crisis**
- **Informed, compliant payment options**
- **Threat actor intel & attribution to help incident response**